INTERFACES CIENTÍFICAS

EXATAS E TECNOLÓGICAS

ISSN IMPRESSO - 2359-4934

ISSN ELETRÔNICO - 2359-4942

DOI - 10.17564/2359-4934.2015v1n2p85-96

SEGURANÇA EM REDES DE COMPUTADORES UMA VISÃO SOBRE O PROCESSO DE PENTEST

Pablo Marques Menezes[1]

Lanay M. Cardoso[2]

Fabio Gomes Rocha[3]

RESUMO

Apesar de existirem normas e procedimentos de boas práticas amplamente discutidas e aceitas a respeito da segurança da informação e sendo implantadas não é garantia que o perigo foi afastado. Após os mecanismos levantados pelos responsáveis pela segurança da informação tenham sido implantados é necessário uma auditoria e testes para garantir que estes estejam de acordo com o a política e que sejam eficazes. Analisaremos as ferramentas e procedimentos para testar a eficiência dos mecanismos de segurança implantados, procedimento denominado de Pentest.

PALAVRAS-CHAVE

Teste de segurança, PenTest, ferramentas de segurança.

ABSTRACT

Although there are rules and procedures widely discussed best practices and accepted about information security and being implemented it is no guarantee that the danger has been removed. After the mechanisms raised by those responsible for information security have been implanted an audit and testing is necessary to ensure that they comply with the the policy and are effective. We will review the tools and procedures for testing the efficiency of implemented security mechanisms, procedure known as Pentest.

KEYWORDS

Safety Test. PenTest. Security Tools.

RESUMEN

Si bien existen normas y procedimientos ampliamente discutidas las mejores prácticas y con respecto a la seguridad de información aceptados y están implementando es ninguna garantía de que el peligro se ha eliminado. Después de que los mecanismos planteados por los responsables de la seguridad de la información se han desplegado una auditoría y las pruebas es necesario asegurarse de que cumplen con la política y son eficaces. Vamos a revisar las herramientas y procedimientos para probar la eficacia de los mecanismos de seguridad implementados, procedimiento llamado Pentest.

PALABRAS CLAVE

prueba de seguridad, PenTest, herramientas de seguridad

1 INTRODUÇÃO

A preocupação com a segurança dos ativos de uma organização no âmbito digital ao fato que de alguma maneira as empresas estão expostas, tal situação implica em investimentos por parte das organizações e elaboração de normas pelos comitês e governos para auxiliar na implantação de mecanismos para que se possa mitigar ou reduzir a níveis aceitáveis as ameaças virtuais.

A análise de segurança da informação em empresas sempre foi uma tarefa muito árdua, pois para manter os dados em segurança é necessária a utilização de uma boa infraestrutura de software para ajudar na análise da rede, sistemas de monitoramento e de testes de rede.

O processo de Auditoria torna-se indispensável na gestão da segurança da informação, pois já que é por meio deste processo consegue-se manter a conformidade com a política de segurança aprovada pelos gestores responsáveis, diante dos recursos e atividades que estão sendo realizados, sendo acompanhado por um responsável que consiga detectar o que precisa ser modificado e o que deve continuar a ser utilizado, avaliando também os riscos que já existem e os que podem vir a existir futuramente.

Sabendo-se que existem duas divisões de Auditoria: Auditoria de Documentação e Auditoria de Certificação. Esta prática hoje em dia pode ser aplicada principalmente em relação à Computação nas Nuvens que vem crescendo, mas trazendo consigo fragilidades, onde todo e qualquer sistema que se encontra com dados e informações na internet ficam sujeitos a qualquer tipo de invasão e inseminação de vírus para derrubar o sistema e ou adquirir conteúdos sigilos e internos.

O termo *Pentest* ou *pentetration* test é um processo que envolve a simulação de ataques reais a riscos associados a potenciais vulnerabilidades, o teste de penetração (pentest) não deve ser confundido com análise de riscos, pois além de descobrir vulnerabilidades irá explorá-la com o objetivo de determinar o impacto no caso de ataque bem sucedido, segundo Potter e McGraw (2004) o testador deve utilizar abordagens baseadas em risco, mas baseado na realidade dos ataques a arquitetura, com uma mentalidade de atacante para medir a segurança do ambiente.

A auditoria de segurança pode ser dividida em duas funções conforme Osborne (1998), uma com o foco na gestão e outra com o foco técnico, interessado em examinar as vulnerabilidades por meio de ferramentas e modelos de validação de segurança, assim através do manuseio e utilização de ferramentas que são escolhidas para que sejam realizados os testes, pode-se ser utilizado o Kali Linux, distribuição GNU/Linux com foco em testes de segurança e análise forense, é possível detectar as falhas e erros que existentes no ambiente computacional e como explorá-los.

Quando da averiguação do sistema, deve-se, de preferência, haver uma pausa no serviço da empresa, pois o servidor ficará indisponível no momento de teste. É preciso fazer uma anotação detalhada das vulnerabilidades encontradas no sistema, para que possa haver correções posteriormente, tornando com que o sistema fique mais confiável.

É importante ressaltar que as principais normas relativas à Segurança estão aqui expostas para conhecimento e cumprimento das regras citadas pela ABNT, as quais não podem deixar de ser notadas. As normas determinam todos os procedimentos para garantia de que a Segurança que irá ser aplicada em qualquer Organização esteja em cumprimento com a lei, tanto em relação aos integrantes que fazem parte do Comitê de Segurança quanto à adequação dos recursos e dependências.

Como foi analisado que a segurança é um fator importante para assegurar os dados de uma empresa,

assim da empresa com base na análise dos pilares da segurança, segundo as normas NBR/ISO/IEC 27001 e 27002 é necessária para que seja possível obter resultados sobre o status de segurança da rede em uma empresa, tendo a ideal concepção da gestão de segurança da informação, atribuída à perícia, auditoria, teste da rede. Facilitando a busca de melhores informações da segurança, por conta disso a realização do desenvolvimento de um sistema operacional baseado nesses pontos da segurança, facilitará o exame de uma rede empresarial.

A tecnologia existente hoje exibe, por trás de um mundo virtual e atrativo, há indivíduos com grande conhecimento tecnológico, mas com interesses financeiros ou por ego denominados de crackers, ou seja, hacker com objetivos que infringem leis e com resultados danosos aos seus alvos. O objetivo é proteger os sistemas ou evitar ataques que os levem a conseguir informações que sejam de propriedade da organização. Então logicamente o pensamento que é feito por qualquer um é como se prevenir diante destes que podem atacar a qualquer momento e trazer prejuízos e danos irreversíveis. Esta pesquisa utilizou como metodologia a pesquisa bibliográfica e validação de ferramentas com base nas normas NBR/ISO de segurança.

2 SEGURANÇA DA INFORMAÇÃO

Sabendo que nenhum sistema é 100% seguro e que os riscos de ataques cibernéticos crescem muito no mundo da internet, como também existem diversas pessoas interessadas em adquirir informações e dados sigilosos de empresas de grande porte, é analisando estes casos que mostramos e detalhamos como podemos melhorar e garantir uma segurança melhor.

Analisando que é essencial ter uma boa segurança na empresa, devemos analisar os pilares da segurança, segundo a norma da série 27000, com base na norma e na necessidade de obter resultados sobre o status de segurança da rede em uma empresa, fez-se ideal a concepção da gestão de segurança da informação, atribuída a perícia, auditoria, teste da rede, facilitando a busca de melhores informações da segurança, por conta disso a realização do desenvolvimento de um sistema operacional baseado nesses pontos da segurança, facilitará o exame de uma rede empresarial.

O foco principal da Segurança da Informação é proteger o ativo mais importante para o negócio, as informações, devendo assim ser colocado em prática os requisitos responsáveis pela segurança que conforme a NBR/ISO/IEC 27002, são eles: confidencialidade, integridade e disponibilidade; apesar de não ser os únicos pontos importantes da segurança, ao atender os critérios necessários aos pilares da segurança, grande parte da proteção estará garantida (LAURENO, 2005).

A partir do momento que se sabe que o acesso à informação encontra-se restrito a certo público e disponível apenas aos usuários legítimos, onde a informação está certamente protegida contra alterações ou destruições, estando de acordo com as conformidades da norma em destaque. Obedecendo todas as normas vigentes é possível resguardar informações sigilosas.

3 TESTE DE PENETRAÇÃO (PENTEST)

Estes testes de segurança podem, também, ser chamados de testes de penetração, ou então no termo em inglês (Pentest), que significa uma penetração que faz no sistema, onde se descobre as falhas do sistema. O teste de penetração pode ser associado ao um termo mais bruto de forma de ataque, mas com o objetivo de achar falhas, aberturas, rastreando por completo todo o sistema, realizando uma auditoria completa.

O profissional desta área testa formas de invadir e penetrar no sistema, burlando a segurança da organização para descobrir as falhas e erros, fazendo com que o serviço de tal empresa fique indisponível.

Informações podem ser obtidas como, por exemplo, por meio do *Footprint* que é um tipo de ataque, onde o teste busca informações por meio de engenharia social, buscas recursivas ao servidor de nomes.

Para que um teste de segurança seja satisfatório o profissional deve ter o conhecimento avançado em programação, conhecer as ferramentas necessárias para os testes, ter ampla visão de sistemas operacionais e suas funcionalidades, além de saber trabalhar a fundo com servidores e redes.

Os testes têm o objetivo de descobrir o grau de risco que um ataque pode ocasionar em tal vulnerabilidade encontrada no sistema, onde é recomendado o controle de segurança em sistemas mais maduros e qualificados, assim todas as falhas serão exploradas e encontradas. Os testes são direcionados a um sistema alvo, com aprofundamento maior a partir dos primeiros resultados, essas tarefas precisam ter uma análise manual realizada pelo profissional, que podem ser encontradas por suporte de ferramentas de testes, sendo testadas as vulnerabilidades, que é um dos principais passos para orientar e priorizar as atividades de pesquisa da segurança.

Nos testes, o profissional basicamente passa praticamente 90% do tempo buscando informações sobre o alvo, e apenas 10% realizando um ataque. Buscar informações sobre um alvo aumenta consideravelmente a possibilidade de que um ataque seja realizado, o profissional busca muitas informações, por que é a partir das informações, que fica muito mais fácil fazer a invasão, por existir informações que deixam as janelas abertas das falhas do sistema, e quando encontramos facilidade, é só partir para ação para conseguir penetrar no sistema.

Existem várias técnicas que antecipam um teste de segurança, pois antes de testar as vulnerabilidades do sistema, temos que identificar os serviços da rede e analisar as diferentes maneiras para penetração no sistema do servidor. Para que os testes sejam eficazes existem métodos que verificam as possíveis aberturas do sistema, como tais técnicas:

- *Port Scan* (varredura de portas): é um tipo de processo de varredura de portas TCP e UDP do sistema-alvo para descobrir e determinar os serviços que estão sendo executados ou os que estão em estado de escuta. Por esse método é possível descobrir as portas que estão vulneráveis, ou seja, as portas que possam estar abertas. Existem programas chamados de Port Scanner que servem para testar estas portas, um dos *Port* Scanner mais conhecidos é o *Nmap*.

- Engenharia Social: é uma prática realizada por pessoas para obter informações na empresa, onde uma pessoa se passa por chefe de tal empresa para conseguir as informações do sistema, deste ao sistema operacional que a empresa está utilizando até mesmo o ip de algumas máquinas, por meio de um telefonema, explorando a confiança das pessoas.

- Enumerando serviços: esta técnica é utilizada com a ajuda de um Port Scanner, pois, é um tipo de processo que verifica os serviços que estão sendo executados no servidor, onde serão enumerados os serviços.

- Mapeamento de rede: é uma técnica muito importante, é a partir desta técnica que os ataques podem ocorrer, pois o mapeamento é um processo que analisa o sistema-alvo, onde descobrem os dados da rede, os ip's do servidor, a máscara e entre outros dados para facilitar o acesso ao sistema.

- Sniffers (farejadores): os farejadores são tipos de programas que conseguem capturar todo o tráfego que passa em um segmento da rede, ou seja, um computador que esteja infectado com um *sniffer* consegue capturar as informações que passa por ele, geralmente os dados são organizados por protocolos, onde são trafegados por pacotes e estes pacotes podem ser capturados.

As técnicas são alguns passos para facilitar o processo dos testes de segurança, tornando mais

simples na hora do ataque ao sistema, testando até mesmo a falha de alguns funcionários com a engenharia social, análise de uma maneira geral nos dados e processos com alguns programas que são relacionados às técnicas dos testes de segurança. Estas técnicas devem ser aplicadas antes do ataque inicial ao sistema, para conseguir acelerar o processo dos testes de segurança.

4 TESTES DE VULNERABILIADES

As vulnerabilidades às vezes aparecem e passam por nós usuários, como se não importassem, mas, para um profissional desta área, não se pode deixar passar, tem que ser feita a verificação, análise e é preciso tentar corrigir ao máximo todos os defeitos, falhas e erros que possam possibilitar a entrada de usuários maliciosos; muitas vezes o uso indevido de um sistema pode ocasionar problemas graves, pode até ser uma falha de hardware, de software, erros de usuários, mudanças de programas, e até mesmos problemas de telecomunicações, esses tipos de vulnerabilidades podem passar despercebidas, e podem gerar danos que alcançam milhões e milhões de perdas financeiras para uma empresa, para isso precisamos detalhar todas as vulnerabilidades que podem ocasionar algum problema.

Os testes que são realizados por métodos padrões e seguem as normas, possuem vantagens, pois aplicará uma metodologia previamente elaborada e analisada, onde o profissional seguirá um caminho certo, baseado nas melhores práticas, as ordens de execução das ações bem como os elementos utilizados já serão conhecidas, assim será mais fácil prever e evitar erros.

Entre os métodos de teste de segurança existe três que merecem destaque especial, que são:

- A metodologia de teste de segurança em aplicações Web do projeto *Open Web Application Security Project* (OWASP) (AGUILERA; ET AL., 2007);

- A OSSTMM – *Open Source Security Testing Methodology Manual* (HERZOG, 2003) mantida por *Institute for Security and Open Methodologies* (ISECOM);

- A ISSAF – *Information Systems Security Assessment Framework* (LEONHARDT,2010), mantida pelo *Open Information Systems Security Group* (OISSG).

Esses são alguns métodos de ferramentas que podem ser usadaos em conjunto para trazer resultados satisfatórios na avaliação de vulnerabilidades.

5 NORMAS DE FACILIDADE PARA TESTES

Sabendo que devemos levar em conta as principais normas de segurança da informação da série ISO/IEC 27000 que foram reservadas para tratar de padrões de segurança da informação, e fazer com que um serviço de uma empresa continue auxiliando seus clientes é necessário seguir os padrões, onde o serviço desta empresa deve conter a (ABNT):

- Confidencialidade - que um arquivo ou documento seja só visto ou editado por devidas pessoas permitidas, onde o acesso à informação seja limitado, e que só o proprietário possa autorizar a informação.

- Integridade – o que é fornecido deve ter as mesmas características originais, sem falhas, e falta de características da informação, incluído o controle de mudanças do ciclo de vida do documento.

- Disponibilidade – é a informação que sempre esteja disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Ao atender os pontos citados acima a empresa garante segurança dos seus ativos e infraestrutura, entretanto para manter alinhadas as estratégias que garantem os pilares da segurança da informação o trabalho deve ser continuo, conforme relatado por Cicco (2008), seguindo a metodologia PDCA (Plan

- do - check - act) planeje, faça, teste e aja. O teste de segurança vai auxiliar a tomar ações e reavaliar as estratégias, além de que os avanços tecnológicos proporcionam novos serviços e assim novas vulnerabilidades é evidente a importância do teste de segurança. Portanto, há uma necessidade de o profissional que é contratado para simular ataques ao sistema da empresa, que este tenha conhecimento das normas, técnicas de ataques, profundo conhecimento de redes, serviços de rede e engenharia social.

6 TIPOS DE ATAQUES

Um dos principais ataques para testes de penetração em um sistema é o ataque de negação de serviço Nakamura (2007), ou seja, o chamado Dos, este tipo de ataque é um teste para saber se o servidor está preparado para este tipo de ataque, que força o sistema a reinicializar até consumir todos os recursos de processamento e memória, de forma que ele não possa mais fornecer o serviço.

Existe além do ataque de negação de serviço, o ataque distribuído que se chama DDoS, que consiste em um ataque que infecta vários computadores, que se tornam "zumbis", que são comandados pelo computador "mestre", onde acessam um serviço todos os computadores na mesma hora, fazendo com que o número limitado de usuários, que o servidor atende simultaneamente nos 'slots' acabem e o servidor não seja capaz de atender a mais nenhum pedido, fazendo com que haja um travamento.

Além destes ataques existe o ataque de força bruta, que consiste na tentativa de adivinhar a senha e o nome do usuário, que significa tentar adivinhar o conjunto por meio de tentativa e erro. Após isso se tenta invadir o sistema, para então descobrir a senha dos usuários que possuem conta no servidor.

Essas técnicas são usadas remotamente principalmente para descobrir senhas de serviços que usam os protocolos POP3, SSH, FTP, TELNET, SMB. Também, existem ferramentas automatizadas para *pentest*, que na maioria das vezes são pagas, e muito caras, mas, que satisfazem muito as organizações por serem fáceis e mais práticas, para realizar o teste de penetração.

Falhas em servidores mal configurados acontecem muitas vezes em empresas o que causa as intrusões de hackers mais facilmente, por isso que o teste de penetração ajuda a observar este ponto.

Podemos atacar por Intrusão de sistema, onde os ataques acontecem por "Buffer Overflow", ou seja, quando o tamanho do buffer do servidor ultrapassa sua capacidade de armazenamento. Verificando que o ataque não dá acesso de root (administrador do sistema) ao atacante. Então ataques baseados em elevação de privilégio buscam dar acesso de root a um atacante que possua apenas um acesso de usuário no servidor.

Entre esses ataques citados, existem vários outros que servem para ajudar no teste de penetração, e que auxiliam os profissionais desta área.

7 AS DESVANTAGENS DOS TESTES DE SEGURANÇA

Quando falamos em teste de segurança, é quando o profissional vai tentar invadir, como se fosse um cracker, então no momento em que isso está ocorrendo, o serviço pode parar, deixando o serviço inacessível, paralisando o sistema, forçando e fazendo com que o sistema reinicie.

8 AS VANTAGENS DOS TESTES DE SEGURANÇA

A vantagem é que se houver algum erro, alguma falha esse será o momento para corrigir antes que uma pessoa mal intencionada prejudique o sistema da sua empresa.

Como a citação acima afirma, a empresa que faz o teste de penetração tem mais confiança e se-

gurança, pois conhece suas falhas, e já corrigiu as possíveis falhas.

Se uma empresa não adere ao teste de segurança, e se o seu sistema possivelmente for atacado e seus dados mais importantes forem roubados, a comunicação na empresa será danificada por conta disso, imagina a perda financeira desta empresa. Muitas empresas acham que não é necessário fazer o teste de segurança, achando que está totalmente protegida, mas, sabemos que nenhum sistema é 100% seguro e protegido, por essa razão é necessário verificar e comprovar que a segurança é realmente eficaz.

Tem empresas acreditando que porque o sistema está funcionando bem, não há a necessidade de avaliá-lo, mas, infelizmente, esta forma de pensar só prejudica; realmente têm que se prevenir dos ataques. As empresas imaginam que o termo segurança, é basicamente ter um programa de antivírus instalado no computador e às vezes ter alguns cuidados com pendrives infectados, conhecidos como os maiores vetores de disseminação de malwares. Sabemos que cuidados como estes são realmente proveitosos, mas não é o bastante, pois com o avanço da tecnologia, muitas pessoas estão evoluídas no sentido tecnológico e vão surgindo novos crackers com o passar do tempo. As seguranças comuns, não é o ideal para que o sistema da empresa ou até mesmo o servidor, estejam totalmente protegidos.

Depois de todas essas informações fica claro que o *pentest* ou testes de segurança, é muito essencial para as organizações, além de ser uma forma de proteção prática e também teórica, que é carregado de normas e certificações sobre segurança, e bem-conceituado pelo mundo. Aquele que sabe tanto se proteger quanto também atacar, esse profissional é considerado um dos melhores na sua área, para conseguir ajudar a trazer as soluções.

Os testes de segurança além de prevenir e organizar os dados da empresa, ajuda no detalhamento do sistema, para ter um conhecimento melhor sobre as portas de entrada do sistema, dos dados em gerais, e de todos os métodos possíveis de prevenção dos arquivos, dados e informações, visando também aplicar as devidas normas de segurança.

9 FERRAMENTAS PARA O TESTE DE SEGURANÇA

Para que o teste de segurança seja feito a pessoa precisa ter um amplo conhecimento nos protocolos de rede, saber como utilizá-los e como empregá-los nas ferramentas que são utilizadas no teste.

Protocolo de rede é um tipo de linguagem na qual os computadores se comunicam, e para entender está comunicação entre eles, precisamos entender estes protocolos, para sabermos lidar com as informações que passam de um computador para o outro. A principal pilha de protocolos e a TCP/IP, sem esses protocolos o computador seria incapaz de se comunicar com a rede, e com outros computadores.

Na pilha de protocolos do TCP/IP, consistem as seguintes camadas, FOROUZAN(2006):

- Na camada de aplicação estão os protocolos de rede HTTP/FTP/TELNET/POP3, sendo estes protocolos responsáveis pelo suporte dos programas;

- Na camada de transporte os protocolos mais utilizados são TCP/UDP, responsáveis pelo envio de pacotes por conexão 'segura' ou 'não segura' respectivamente.

- Na camada de internet os protocolos associados a esta camada são IP/ICMP/ARP/RARP, que são responsáveis pelo endereçamento de pacotes;

- A camada física é responsável pela conversão dos pacotes para sinais eletrônicos, chamado de bits, para prover a conexão física.

Estes protocolos ajudam, quanto à utilização dos programas de segurança, para os testes de segurança, então é preciso entender o funcionamento de cada ferramenta. As ferramentas que serão explicadas servem para fazer tipos de ataques específicos, como: ataque de força bruta, ataque de negação de serviço, "sniffar" a rede, SYN flood, TCP kill e entre outros. Que serão feitos a partir de algumas ferramentas como:

- Ettercap: este programa funciona em meio de ataques na Lan, onde possui *sniffing* de conexões, filtragem de conteúdo, funciona até mesmo em protocolos criptografados, onde tem um recurso de análise de rede e host. Sua versão mais recente é a NG-0.7.3;

- Wireshark: é um programa que analisa os protocolos de rede, examina dados de uma rede ao vivo ou de um arquivo, este programa ajuda muito na hora do teste de penetração;

- Nmap: é um tipo de *scanner* de hosts que usa recursos avançados para verificar o estado do seu alvo.

- Arping: esta ferramenta analisa os hosts em uma rede, o arping é um análogo em função de ping, que utiliza o protocolo ICMP, e também usa o protocolo ARP para sondar hosts.

- Netdiscover: esta ferramenta tem a função de descobrir os endereços da rede, onde ela trabalha com o protocolo ARP, que envia requisições e fareja respostas.

- Hping: é uma ferramenta muito poderosa, existem três vias que possibilitam o ataque, para negação de serviço, conhecidas como SYN, SYN/ACK e ACK, sendo que o objetivo principal é fazer com que o computador não responda a todas as requisições que serão enviadas, acontecendo um desprezo diante dos pacotes SYN.

- Netstat: esta ferramenta torna-se bastante interessante, já que permite ver as conexões que um determinado host está abrindo, e também descobrir erros na rede.

Estas ferramentas citadas servem tanto para rastreamento de hosts, ou seja, análise de computadores na rede, como também para fazer ataques de negação de serviço, ataque de força bruta, rastreamento de dados e arquivos, análise de e-mails e senhas e entre outros focos de penetração da rede.

Em uma análise geral sobre algumas informações e as principais ferramentas utilizadas para os testes, sabemos que além de ter uma importância no trabalho em geral, devemos lembrar que as ferramentas fazem parte do conjunto de métodos para que o teste de segurança em si, seja realizado, lembrando que estas ferramentas estão associadas à remasterização de um sistema operacional, utilizado para devidos fins, seguindo as normas, para que não haja erros e falhas no momento dos testes.

Existem algumas ferramentas para verificar a força da senha dos usuários, estas ferramentas auxiliam na segurança das senhas na empresa, além destes programas que ajudam tem outros métodos, como o numero de dígitos acima de oito, não colocar nome da pessoa, ou de parentes nas senhas, palavras comuns, pois, pode ser um risco para a empresa, devendo ter um cuidado sobre a força da senha. Para verificar a segurança da senha existem ferramentas online para realizar estes testes, tais ferramentas online como:

- Pass Pub;

- Password Chart;

- SafePasswd.

Além de ferramentas on-line, tem programas que podem ser instalados no sistema operacional, como o *Pwgen* que é um utilitário para verificar as senhas, além de fazer senhas mais difíceis, ele faz senhas aleatoriamente de acordo com a dificuldade que a pessoa

deseja, de uso fácil e compreensível para os usuários e até mesmo para os administradores de rede, e é compatível com o Ubuntu, Debian, Fedora e entre outros.

Algumas ferramentas não foram citadas, pois, são pouco usadas no andamento dos testes de segurança, embora possam ser utilizadas para algumas ocasiões dependendo da necessidade, e do foco, mas, neste trabalho, o foco analisado é o rastreamento da rede, e do servidor, analisando portas, e algumas falhas comuns.

10 MÉTODO PARA AUDITORIA DE SEGURANÇA ATRAVÉS DE TESTES

Para manter os ativos de informação seguros o custo torna-se alto, mas preciso. Começando pela Gestão do risco em segurança da informação. As vulnerabilidades e ameaças devem ser detectadas para a procura de soluções, evitando causar fortes impactos que afetem o comprometimento da segurança; com base na realização de processos serão implementadas as medidas de proteção viáveis, e o equilíbrio do custo financeiro e operacional de acordo com a empresa. Para conseguir o controle o risco deve ser julgado dessa forma: avaliação do risco, aceitação do risco e comunicação do risco.

A partir do momento que é feita a identificação do risco ele é classificado, ou seja, se ele foi gerado por fenômenos ambientais, ou por técnicas lógicas e humanas, erro na configuração de componentes de TI, ou falhas de hardware e software.

Sabendo que qualquer informação é valiosa para uma empresa, a responsabilidade entra em jogo, devem ser avaliados os critérios de segurança mais adequados para aplicação, fazendo com que apenas as pessoas de direito tenham acesso e os recursos da informação sejam íntegros e confidenciais, serviço que é prestado por profissionais da área de TI; evitando roubos, fraudes ou vazamentos. Quando se trabalha com dados, servidores, aplicações e equipamentos há a necessidade por controle das atualizações de toda a infraestrutura da empresa, para que não ocorram paradas que deixem o serviço indisponível.

A informação deve ser classificada, mas de um modo evidente e reconhecível para que quem for responsável por recebê-la e compartilhá-la com as áreas de negócio que tenham acesso aos recursos possa entender claramente. É importante que um comitê de segurança faça um mapeamento organizado e gerencie os ativos da melhor forma, sejam eles digitais ou não.

Hoje em dia a tecnologia deu uma grande avançada, em contrapartida é possível perceber que as formas de armazenamento das informações e seus recursos passaram não só a ser armazenadas em banco de dados como antes, elas acabaram migrando também para notebooks, desktops, pendrives, smartphones, CD'S e e-mails, podem até mesmo estarem armazenados na nuvem, caso este que requer maior segurança já que o mundo da internet atrai vários crackers em busca de senhas e acesso a informações do próprio interesse que não são liberadas normalmente ao público.

Vale ressaltar que qualquer transformação no perfil de acesso em relação aos colaboradores deve ser documentada e disposta para futuras consultas, e o cumprimento dos prazos para validar e conceder acessos deve ser feito.

As redes de computadores, e consequentemente a Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (LAUREANO, 2005).

Recentemente o que mais se houve falar é sobre Cloud Computing, (Computação nas nuvens) e para

o bom acesso a essa tecnologia na nuvem a Segurança se torna indispensável, os maiores esforços no desenvolvimento é voltado para o uso da criptografia, mas os usuários que tiverem acesso a este tipo de tecnologia devem ser, também, os responsáveis por estarem preocupados com as suas senhas, atualizando-as.

As redes modernas, baseadas na tecnologia permitem utilizar padrões de internet, onde qualquer indivíduo pode a um custo mais baixo ter acesso a informações localizadas nos mais distantes pontos do país, podendo criar, gerenciar e distribuir informações no mundo de forma prática rápida e fácil. Com base nisso o compartilhamento entre serviços em corporações permite ganho de produtividade.

Contudo é de fácil percepção que todo sistema está sujeito a invasões caso ocorra falha na especificação das condições e controle de acesso, que exploradas por usuários da rede causam grandes impactos de níveis altos e prejudiciais; trazendo desde um simples constrangimento a altas perdas financeiras, que podem ser provocados por queda da rede; como por exemplo, em um site de vendas, uma queda pode fazer com que vários produtos não sejam vendidos em um curto período de tempo.

Entra aí, neste sentido, a segurança; a definição de regras em uma política de segurança, deve ser fundamentada em três questionamentos: O que proteger, de que ou quem proteger e como fazer essa proteção, tendo em vista que a depender das informações e da organização o grau de proteção varia certamente, muitas vezes ocorre de uma informação ser sigilosa para uma empresa e para outra não ter um grau tão elevado de sigilo.

Há vários tipos de ferramentas que colaboram para ataques, existem até mesmo sites na internet dedicados a atividades de hacking, criados com a intenção de buscar falhas no sistema ou configuração, e vulnerabilidades em redes alvo.

A providência cabível para esse tipo de ação baseia-se no objetivo das transações e no que se deve proteger. Lembrando que a Segurança não deve focar apenas no alvo externo da rede, a segurança interna deve prevalecer também, pois funcionários podem ter interesses, devendo ser feito o acesso restrito. Visto que grandes partes dos problemas estão associados a ameaças internas.

Os objetivos de segurança podem variar, dependendo do tipo de informação. O que deve ser verificado, principalmente no ciclo de vida da informação em uma corporação, é a autenticidade, a integridade e a disponibilidade, não precisando estar tão preocupado com a confidencialidade que por vir depois, será de mínima importância nesse momento; segundo um estudo que foi divulgado pela imprensa, a proteção se faz necessária quando quer se prevenir contra alguma alteração que possa ser feita por alguém que se passe por diretor e possa enviar para o setor de divulgação alguma informação que possa prejudicar a empresa, então dessa forma a autenticidade e integridade garante que um comunicado não seja alterado.

Uma vez que exista um documento que será destinado ao público geral, seria necessário se preocupar mais com a autenticidade e irritabilidade da comunicação do emissor descartando do receptor que apenas quer o aceitamento do comunicado corretamente.

Em uma organização é preciso dar início ao processo, identificando as necessidades e requisitos da informação, tratamento, distribuição, coleta contínua, devendo alimentar os processos decisórios e operacionais e levar após isso as informações para o ambiente externo (BÖHME, 2010).

Caso a confiança que se tenha, acreditando que os dados estejam protegidos, seja destruída, o impacto causado certamente implicará na destruição do sistema.

Para manter os ativos de informação o custo se torna alto, mas preciso. Começando pela Gestão do risco

em segurança da informação. As vulnerabilidades e ameaças devem ser detectadas para a procura de soluções, evitando causar fortes impactos que afetem o comprometimento da segurança; com base na realização de processos serão implementadas as medidas de proteção viáveis, e o equilíbrio do custo financeiro e operacional de acordo com a empresa. Para conseguir o controle, o risco deve ser julgado dessa forma: avaliação do risco, aceitação do risco e comunicação do risco.

A partir do momento que é feita a identificação do risco ele é classificado, ou seja, se ele foi gerado por fenômenos ambientais, ou por técnicas lógicas e humanas, erro na configuração de componentes de TI, ou falhas de hardware e software.

11 CONCLUSÃO

É imprescindível que em uma empresa haja, frequentemente, uma análise em seu sistema, com as ferramentas para a verificação do sistema, com o foco de proteger as informações que estão no servidor, devendo proteger os serviços prestados e estando ligado junto as normas que, também, devem ser respeitadas para haver um acordo não infringindo as normas de segurança e obedecendo as principais. Para conciliar as normas com os devidos testes de segurança, devendo colocar em prática o que foi analisado e escrito, com as ferramentas do sistema criado, deve-se corresponder aos requisitos responsáveis pela segurança, tais como: confidencialidade, integridade e disponibilidade.

É preciso ressaltar que as principais normas relativas à Segurança, são expostas para o conhecimento e o cumprimento das regras citadas pela ABNT, as quais não podem deixar de ser colocadas. As normas são bases essenciais para o desenvolvimento deste trabalho, pois em uma empresa os serviços nela prestados devem obedecer a tais normas, onde o cumprimento das mesmas é associado ao sistema operacional remasterizado para os devidos fins, existindo assim um gerenciamento das informações que trafegam no sistema.

REFERÊNCIAS

ABNT. **Tecnologia da informação**. Técnicas de segurança. Código paragestão de segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

BÖHME, Rainer; FÉLEGYHÁZI, Márk. Optimal information security investment with penetration testing. **Decision and Game Theory for Security**. Springer Berlin Heidelberg, 2010. p.21-37.

CICCO, Francesco D. A nova norma internacional ISO 27005 de gestão de riscos de segurança da informação. **QSP**. Disponível em: <http://www.qsp.org.br/artigo_27005.shtml>. Acesso em: 24 jan. 2015

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. São Paulo: Mcgraw Hill Brasil, 2006.

HERZOG, Pete. Open-source security testing methodology manual. **Institute for Security and Open Methodologies (ISECOM)**, 2003.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>.
Acesso em: 10 nov. 2014.

LEONHARDT, FRANK. AUDITING, PENETRATION TESTING AND ETHICAL HACKING. **Handbook of electronic security and digital forensics**, 2010. p.93.

NAKAMURA, Emilio Tassato. **Segurança de redes**: em ambientes cooperativos. São Paulo: Novatec, 2007.

OSBORNE, K. Auditing The IT Security Function. **Revista Computers & Security**, 17, 1998. p.34-41.

POTTER, B; MCGRAW, G. Software security testing. **Revista IEEE SECURITY & PRIVACY**, 2/5, 2004. p.81-85.

1 Mestrando em Computação – Universidade Federal de Sergipe (UFS). E-mail: menezes.pmm@gmail.com
2 Graduanda em Sistemas de Informação - Universidade Tiradentes (Unit) – Aracaju, SE – Brasil. E-mail: marqueslanay@gmail.com
3 Mestrando em Computação (UFS), Professor de Computação da Universidade Tiradentes (Unit) – Aracaju, SE – Brasil. E-mail: gomesrocha@gmail.com

Recebido em: 8 de Março de 2015
Avaliado em: 10 de Março 2015
Aceito em: 4 de Abril de 2015